Douglas S. Swetnam (IN State Bar #15860-49)
Section Chief – Data Privacy & ID Theft Unit
Office of Attorney General Curtis Hill Jr.
302 W. Washington St., 5th Floor
Indianapolis, IN 46204
Email: douglas.swetnam@atg.in.gov
Telephone: (317) 232-6294

Michael A. Eades (IN State Bar #31015-49)
Deputy Attorney General
Office of Attorney General Curtis Hill, Jr.
302 W. Washington St., 5th Floor
Indianapolis, IN 46204
Email: Michael.Eades@atg.in.gov
Telephone: (317) 234-6681

John C. Gray (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Mark Brnovich
2005 N. Central Ave.
Phoenix, AZ 85004
Email: John.Gray@azag.gov
Telephone: (602) 542-7753
Attorney for Plaintiff State of Arizona

Peggy Johnson (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Leslie Rutledge
323 Center St., Suite 200
Little Rock, AR 72201
Email: peggy.johnson@arkansasag.gov
Telephone: (501) 682-8062
Attorney for Plaintiff State of Arkansas

Michele Lucan (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General William Tong
110 Sherman Street
Hartford, CT 06105
Email: michele.lucan@ct.gov
Telephone: (860) 808-5440
Attorney for Plaintiff State of Connecticut

Patrice Malloy (Pro Hac Vice)
Bureau Chief, Multistate and Privacy Bureau
Florida Office of the Attorney General
110 SE 6th Street
Fort Lauderdale, FL 33301
(954) 712-4669
Patrice.Malloy@myfloridalegal.com

Diane Oates (Pro Hac Vice)
Assistant Attorney General
Florida Office of the Attorney General
110 Southeast 6th Street
Fort Lauderdale, FL 33301
Email: Diane.Oates@myfloridalegal.com
Telephone: (954) 712-4603
Attorneys for Plaintiff State of Florida

William Pearson (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Tom Miller
1305 E. Walnut, 2nd Floor
Des Moines, IA 50319
Email: William.Pearson@ag.iowa.gov
Telephone: (515) 281-3731
Attorney for Plaintiff State of Iowa

Sarah Dietz (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Derek Schmidt
120 S.W. 10th Ave., 2nd Floor
Topeka, KS 66612
Email: sarah.dietz@ag.ks.gov
Telephone: (785) 368-6204
Attorney for Plaintiff State of Kansas

Kevin R. Winstead (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Andy Beshear
1024 Capital Center Drive
Frankfort, KY 40601
Email: Kevin.Winstead@ky.gov
Telephone: (502) 696-5389
Attorney for Plaintiff Commonwealth of Kentucky

Alberto A. De Puy (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Jeff Landry
1885 N. Third St.
Baton Rouge, LA 70802
Email: DePuyA@ag.louisiana.gov
Telephone: (225) 326-6471

L. Christopher Styron (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Jeff Landry
1885 N. Third St.
Baton Rouge, LA 70802
Email: styronl@ag.louisiana.gov
Telephone: (225) 326-6400
Attorneys for Plaintiff State of Louisiana

Kathy Fitzgerald (Pro Hac Vice)
Assistant Attorney General
Department of Attorney General Dana Nessel
Corporate Oversight Division
525 W. Ottawa St., 5th Floor
Lansing, MI 48933
Email: fitzgeraldk@michigan.gov
Telephone: (517) 335-7632
Attorney for Plaintiff State of Michigan

Jason T. Pleggenkuhle (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Keith Ellison
Bremer Tower, Suite 1200
445 Minnesota St.
St. Paul, MN 55101-2130
Email: jason.pleggenkuhle@ag.state.mn.us
Telephone: (651) 757-1147
Attorney for Plaintiff State of Minnesota

Daniel J. Birdsall (Pro Hac Vice)
Assistant Attorneys General
Office of Attorney General Doug Peterson
2115 State Capitol
PO Box 98920
Lincoln, NE 68509
Email: dan.birdsall@nebraska.gov
Telephone: (402) 471-1279
Attorney for Plaintiff State of Nebraska

Kimberley A. D'Arruda (Pro Hac Vice)
Special Deputy Attorney General
North Carolina Department of Justice
Office of Attorney General Joshua H. Stein
P.O. Box 629
Raleigh, NC 27602-0629
Email: kdarruda@ncdoj.gov
Telephone: (919) 716-6013
Attorney for Plaintiff State of North Carolina

Carolyn U. Smith (Pro Hac Vice)
Senior Assistant Attorney General
Office of the Attorney General and Reporter Herbert H. Slatery III
P.O. Box 20207
Nashville, TN 37202-0207
Email: carolyn.smith@ag.tn.gov
Telephone: (615) 532-2578
Attorney for Plaintiff State of Tennessee

Tanya L. Godfrey (Pro Hac Vice)
Assistant Attorney General
Office of the West Virginia Attorney General Patrick Morrisey
269 Aikens Center
Martinsburg, WV 25404
Email: tanya.l.godfrey@wvago.gov
Telephone: (304) 267-0239
Attorney for Plaintiff State of West Virginia

R. Duane Harlow (Pro Hac Vice)
Assistant Attorney General
Director, Consumer Protection and Antitrust Unit
Wisconsin Department of Justice
Office of Attorney General Josh Kaul
17 W. Main St., P.O. Box 7857
Madison, WI 53707-7857
Email: HarlowRD@doj.state.wi.us
Telephone: (608) 266-2950
Attorney for Plaintiff State of Wisconsin

**IN THE UNITED STATES DISTRICT COURT**
**FOR THE NORTHERN DISTRICT OF INDIANA**
**SOUTH BEND DIVISION**

| | |
|---|---|
| The States of Arizona; Arkansas; Connecticut; Florida; Indiana; Iowa; Kansas; Kentucky; Louisiana; Michigan; Minnesota; Nebraska; North Carolina; Tennessee; West Virginia; and Wisconsin,<br><br>Plaintiffs;<br><br>v.<br><br>Medical Informatics Engineering, Inc. d/b/a Enterprise Health, LLC and K&L Holdings, and NoMoreClipboard, LLC,<br><br>Defendants. | Case No.:3:18-cv-969-RLM-MGG |

**AMENDED COMPLAINT**

Plaintiffs, the states of Arizona, Arkansas, Connecticut, Florida, Indiana, Iowa, Kansas, Kentucky, Louisiana, Michigan, Minnesota, Nebraska, North Carolina, Tennessee, West Virginia, and Wisconsin (collectively "Plaintiff States"), for their complaint against Defendants Medical Informatics Engineering, Inc., ("MIE") operating as Enterprise Health, LLC and K&L Holdings, and NoMoreClipboard, LLC, ("NMC" together with MIE "Defendants"), allege:

## SUMMARY OF THE CASE

1. Intermittently between May 7, 2015 and May 26, 2015, unauthorized persons ("hackers") infiltrated and accessed the inadequately protected computer systems of Defendants. During this time, the hackers were able to access and exfiltrate the electronic Protected Health Information ("ePHI"), as defined by 45 C.F.R. § 160.103, of 3.9 million individuals, whose PHI was contained in an electronic medical record stored in Defendants' computer systems. Such

personal information obtained by the hackers included names, telephone numbers, mailing addresses, usernames, hashed passwords, security questions and answers, spousal information (names and potentially dates of birth), email addresses, dates of birth, and Social Security Numbers. The health information obtained by the hackers included lab results, health insurance policy information, diagnosis, disability codes, doctors' names, medical conditions, and children's name and birth statistics.

2. In fostering a security framework that allowed such an incident to occur, Defendants failed to take adequate and reasonable measures to ensure their computer systems were protected, failed to take reasonably available steps to prevent the breaches, failed to disclose material facts regarding the inadequacy of their computer systems and security procedures to properly safeguard patients' personal health information, failed to honor their promises and representations that patients' personal health information would be protected, and failed to provide timely and adequate notice of the incident, which caused significant harm to consumers across the United States.

3. Defendants' actions resulted in the violation of the state consumer protection, data breach, personal information protection laws and federal HIPAA statutes, as more fully outlined below. Plaintiffs seek to enforce said laws by bringing this action.

4. This action is brought, in their representative and individual capacities as provided by state and federal law, by the attorneys general of Arizona, Arkansas, Connecticut, Florida, Indiana, Iowa, Kansas, Kentucky, Louisiana, Michigan, Minnesota, Nebraska, North Carolina, Tennessee, West Virginia, and Wisconsin (collectively the "Attorneys General"). The plaintiffs identified in the paragraph are also referred to collectively as the "Plaintiff States."

5. The Plaintiff States bring this action pursuant to consumer protection, business regulation, and/or data security oversight authority conferred on their attorneys general, secretaries of state, and/or state agencies by state law, federal law, and/or pursuant to *parens patriae* and/or common law authority. These state laws authorize the Plaintiff States to seek temporary, preliminary, and permanent injunctive relief, civil penalties, attorneys' fees, expenses, costs, and such other relief to which the Plaintiff States may be entitled.

6. This action is also brought by the Attorneys General of the Plaintiff States pursuant to the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act, 42 U.S.C. § 1302(a), and the Department of Health and Human Services Regulations, 45 C.F.R. § 160 *et seq.*(collectively, "HIPAA"), which authorize attorneys general to initiate federal district court proceedings and seek to enjoin violations of, and enforce compliance with HIPAA, to obtain damages, restitution, and other compensation, and to obtain such further and other relief as the court may deem appropriate.

## JURISDICTION AND VENUE

7. This Court has jurisdiction over the federal law claims pursuant to 42 U.S.C. § 1320d-5(d), and 28 U.S.C. §§ 1331 and 1337(a). This Court has supplemental jurisdiction over the subject matter of the state law claims pursuant to 28 U.S.C. § 1367.

8. Venue in this District is proper pursuant to 28 U.S.C. §§ 1391(b) and (c).

9. The Attorneys General provided prior written notice of this action to the Secretary of HHS, as required by 42 U.S.C. § 1320d-5(d)(4). The Attorneys General have also provided a copy of this complaint to the Secretary of HHS. *Id.*

10. At all times relevant to this matter, Defendants were engaged in trade and commerce affecting consumers in the States insofar as Defendants provided electronic health records services to health care providers in the States. Defendants also maintained a website for patients and client health care providers in the States.

**PLAINTIFFS**

11. The Attorneys General are charged with, among other things, enforcement of the Deceptive Trade Practices Acts, the Personal Information Protection Acts, and the Breach Notification Acts. The Attorneys General, pursuant to 42 U.S.C. § 1320d-5(d), may also enforce HIPAA.

12. The Attorneys General are the chief legal officers for their respective states and commonwealths. The Plaintiff States bring this action pursuant to consumer protection, business regulation, and/or data security oversight authority conferred on their attorneys general, secretaries of state, and/or state agencies by state law, federal law, and/or pursuant to *parens patriae* and/or common law authority.

13. Plaintiff Attorneys General institute this action for injunctive relief, statutory damages, attorney fees, and the costs of this action against Defendants for violations of the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act, 42 U.S.C. § 1302(a), and the Department of Health and Human Services Regulations, 45 C.F.R. § 160 *et seq.*(collectively, "HIPAA"), and supplemental state law claims under Plaintiffs' respective Unfair, Deceptive, or Abusive Acts or Practices ("UDAP") statutes, Disclosure of Data Breach

Statutes (also referred to as "Breach Notification Acts"), and Personal Information Protection Statutes (also referred to as "PIPA"), specifically:

| State | Deceptive Acts | Data Breach | PIPA |
|---|---|---|---|
| Arizona: | Ariz. Rev. Stat. § 44-1521 et seq. | | |
| Arkansas: | Ark. Code § 4-88-101 *et seq.* | Ark. Code § 4-110-105 | Ark. Code § 4-110-101 *et seq.* |
| Connecticut: | Conn. Gen. Stat. § 42-110b *et seq.* | Conn. Gen. Stat. § 36a-701b | Conn. Gen. Stat. § 42-471 |
| Florida: | Chapter 501, Part II, Florida Statutes | Section 501.171, Florida Statutes | Section 501.171, Florida Statutes |
| Indiana: | Ind. Code §§ 24-5-0.5-4(C), and 24-5-0.5-4(G) | | Ind. Code § 24-4.9-3-3.5(f) |
| Iowa: | Iowa Code § 714.16 | Iowa Code § 715c.2 | |
| Kansas: | Kan. Stat. §§ 50-632, and 50-636 | Kan. Stat. § 50-7a02 | Kan. Stat. § 50-6139b |
| Kentucky: | Ky. Rev. Stat. §§ 367.110-.300, and 367.990 | | |
| Louisiana: | La. Rev. Stat. § 51:1401 et seq. | La. Rev. Stat. 51:3071 et seq. | |
| Michigan: | Mich. Comp. Laws § 445.901 *et seq.* | Mich. Comp. Laws § 445.72(13) | |
| Minnesota: | Minn. Stat. §§ 325D.43 *et seq.*; Minn. Stat. §§ 325F.68 *et seq.* | Minn. Stat. § 325E.61 | |
| Nebraska: | Neb. Rev. Stat. §§ 59-1602; 59-1608, 59-1614, and 87-302 | Neb. Rev. Stat. § 87-806 | |
| North Carolina | N.C. Gen. Stat. § 75-1.1, *et seq.* | N.C. Gen. Stat. § 75-65 | N.C. Gen. Stat. § 75-60, *et seq.* |
| Tennessee: | Tenn. Code Ann. § 47-18-101 *et seq.* | Tenn. Cod Ann. § 47-18-2107 | Tenn. Code Ann. § 47-18-2110 |
| West Virginia: | W.Va. Code §§ 46A-1-101 *et seq.*, 46A-7-108, and 46A-7-111 | | |
| Wisconsin: | Wis. Stat. §§ 93.20, 100.18, and 100.26 | Wis. Stat. § 134.98 | Wis. Stat. §§ 146.82 and 146.84(2)(b) |

## DEFENDANTS

14. Defendant MIE is a citizen of the State of Indiana. MIE is a corporation that is incorporated in Indiana and has its principal place of business in Indiana at 6302 Constitution Drive, Fort Wayne, IN 46804.

15. Defendant NMC is a citizen of the State of Indiana. NMC is a wholly-owned subsidiary of MIE, is organized in Indiana, and has its principal place of business in Indiana at 6312 Constitution Drive, Fort Wayne, IN 46804.

16. Prior to January 6, 2016, MIE also operated under the name of Enterprise Health. Enterprise Health was a division of MIE. On January 6, 2016, MIE formed Enterprise Health, LLC, which shares founders, officers, employees, offices, and servers with MIE and NMC.

17. K&L Holdings, LLC is affiliated with MIE and has the same founders, officers, and occupies the same offices as MIE, NMC, and Enterprise Health. K&L Holdings, LLC owns the property that serves as the headquarters for K&L Holdings, LLC, MIE, NMC, and Enterprise Health.

## FACTUAL ALLEGATIONS

18. MIE is a third-party provider that licenses a web-based electronic health record application, known as WebChart, to healthcare providers. MIE, through its subsidiary NMC, also provides patient portal and personal health records services to healthcare providers that enable

patients to access and manage their electronic health records. Through its WebChart application, MIE provides electronic health services to physicians and medical facilities nationwide.

19. At all relevant times, MIE's customers consisted of healthcare providers who were Covered Entities within the meaning of HIPAA. 45 C.F.R. § 160.103.

20. At all relevant times, MIE and NMC were Business Associates within the meaning of HIPAA. 45 C.F.R. § 160.103.

21. As Business Associates, Defendants are required to comply with the HIPAA federal standards that govern the security of ePHI, including Security Rules. *See* 45 C.F.R. § 164.302.

22. The Security Rule generally prohibits Covered Entities and Business Associates, such as Defendants, from unlawfully disclosing ePHI. The Security Rule requires Covered Entities and Business Associates to employ appropriate Administrative, Physical, and Technical Safeguards to maintain the security and integrity of ePHI. *See* 45 C.F.R. § 164.302.

23. At all relevant times, no written agreement existed between MIE and its subsidiary NMC to appropriately safeguard the information created, received, maintained, or transmitted by the entities.

24. Between May 7, 2015 and May 26, 2015, hackers infiltrated and accessed the computer systems of Defendants.

25. The hackers stole the ePHI of 3.9 million individuals whose health information was contained in an electronic medical records database stored on Defendants' computer systems.

26. On June 10, 2015, MIE announced a "data security compromise that has affected the security of some personal and protected health information relating to certain clients and

individuals who have used a Medical Informatics Engineering electronic health record." *Medical Informatics Engineering Updates Notice to Individuals of Data Security Compromise,* MIE (July 23, 2015), http://www.mieweb.com/notice.

27. On June 20, 2015, NMC announced "a data security compromise that has affected the security of some personal and protected health information relating to individuals who have used a NoMoreClipboard personal health record or patient portal." *NoMoreClipboard Notice to Individuals of a Data Security Compromise*, NoMoreClipboard (July 23, 2015), https://www.nomoreclipboard.com/notice.

28. Defendants admitted that unauthorized access to their network began on May 7, 2015, but they did not discover the suspicious activity until May 26, 2015.

29. After discovering the intrusion, Defendants "began an investigation to identify and remediate any identified security vulnerability," hired "a team of third-party experts to investigate the attack and enhance data security and protection," and "reported this incident to law enforcement including the FBI Cyber Squad." *MIE Notice*, http://www.mieweb.com/notice; *NoMoreClipboard Notice*, https://www.nomoreclipboard.com/notice.

30. MIE admitted that the following information was accessed by the hackers: "an individual's name, telephone number, mailing address, username, hashed password, security question and answer, spousal information (name and potentially date of birth), email address, date of birth, Social Security number, lab results, health insurance policy information, diagnosis, disability code, doctor's name, medical conditions, and child's name and birth statistics." *MIE Notice*, http://www.mieweb.com/notice.

31. NMC admitted that the following information was accessed by the hackers: "an individuals' [sic] name, home address, Social Security number, username, hashed password,

spousal information (name and potentially date of birth), security question and answer, email address, date of birth, health information, and health insurance policy information." *NoMoreClipboard Notice*, https://www.nomoreclipboard.com/notice.

32. Defendants began notifying affected individuals by mail on July 17, 2015. This was two months after the initial breach date of May 7, 2015, and over 50 days after the breach discovery date of May 26, 2015.

33. Defendants did not conclude mailing notification letters until December 2015, six months after the breach discovery date of May 26, 2015.

34. Defendants' security framework was deficient in several respects. Defendants failed to implement basic industry-accepted data security measures to protect individual's health information from unauthorized access. Specifically, Defendants set up a generic "tester" account which could be accessed by using a shared password called "tester" and a second account called "testing" with a shared password of "testing". In addition to being easily guessed, these generic accounts did not require a unique user identification and password in order to gain remote access. In a formal penetration test conducted by Digital Defense in January 2015, these accounts were identified as high risk, yet Defendants continued to employ the use of these accounts and, in fact, acknowledged establishing the generic accounts at the request of one of its' health care provider clients so that employees did not have to log-in with a unique user identification and password.

35. Defendants did not have appropriate security safeguards or controls in place to prevent exploitation of vulnerabilities within their system. The "tester" account did not have privileged access but did allow the attacker to submit a continuous string of queries, known as a SQL injection attack, throughout the database as an authorized user. The queries returned error

messages that gave the intruder hints as to why the entry was incorrect, providing valuable insight into the database structure.

36. The vulnerability to an SQL injection attack was identified as a high risk during a penetration test performed by Digital Defense in 2014. Digital Defense recommended that Defendant "take appropriate measures to implement the use of parameterized queries, or ensure the sanitization of user input." The steps taken by Defendants to address this vulnerability were insufficient to mitigate SQL vulnerabilities involved in this incident.

37. The intruder used information gained from the SQL error messages to access the "checkout" account, which had administrative privileges. The "checkout" account was used to access and exfiltrate more than 1.1 million patient records from Defendants' databases. The SQL error exploit was also used to obtain a second privileged account called "dcarlson". The "dcarlson" account was used to access and exfiltrate more than 565,000 additional records that were stored in a database containing NMC patient records.

38. On May 25, 2015, the attacker initiated a second method of attack by inserting malware called a "c99" cell on Defendants' system. This malware caused a massive number of records to be extracted from Defendants' databases. The huge document dump slowed down network performance to such an extent that it triggered a network alarm to the system administrator. The system administrator investigated the event and terminated the malware and data exfiltration on May 26, 2015.

39. Defendant's post-breach response was inadequate and ineffective. While the c99 attack was being investigated, the attacker continued to extract patient records on May 26 and May 28, using the privileged "checkout" credentials acquired through use of the SQL queries. On those two days, a total of 326,000 patient records were accessed.

40. The breach was not successfully contained until May 29, when a security contractor hired by Defendant identified suspicious IP addresses which led the contractor to uncover the principal SQL attack method.

41. Defendants failed to implement and maintain an active security monitoring and alert system to detect and alert on anomalous conditions such as data exfiltration, abnormal administrator activities, and remote system access by unfamiliar or foreign IP addresses. The significance of the absence of these security tools cannot be overstated, as two of the IP addresses used to access Defendants' databases originated from Germany. An active security operations system should have identified remote system access by an unfamiliar IP address and alerted a system administrator to investigate.

42. Defendants' privacy policy, in effect at the time of the breach, stated: "Medical Informatics Engineering uses encryption and authentication tools (password and user identification) to protect your personal information…[O]ur employees are aware that certain information provided by our customers is confidential and is to be protected." Yet Defendants failed to encrypt the sensitive personal information and ePHI within MIE's computer systems, a protection that, had it been employed, would have rendered the data unusable.

43. Defendants' information security policies were deficient and poorly documented. For example, the incident response plan provided by Defendants was incomplete. There are several questions posed in the document that indicate it is still in a coordination or draft stage. Indeed, there is no documented evidence or checklist to indicate that Defendants followed their

own incident response plan. Finally, there is no documentation that Defendants conducted HIPAA Security and Awareness training for 2013, 2014, or 2015, prior to the breach.

44. Defendants' actions caused harm to members of the Plaintiff States. Specifically, the victims are subject to emotional distress due to their personal information and ePHI being in the hands of unknown and untrusted individuals, in addition to the increased potential for harm that could result from instances of fraud.

## DEFENDANTS' LAW VIOLATIONS

### Count I
### Arizona: Violation of HIPAA Safeguards

45. Plaintiff, Arizona, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

46. Defendants' conduct constitutes violations of Administrative Safeguards, Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

a. MIE failed to review and modify security measures needed to continue the provision of reasonable and appropriate protection of ePHI in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.306(e).

b. MIE failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI that it maintained in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

c. MIE failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in accordance with the

implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B).

d. MIE failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and Security Incident tracking reports in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

e. MIE failed to implement policies and procedures that, based upon its access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process that includes ePHI in accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

f. MIE failed to implement policies and procedures to address Security Incidents, including suspected Security Incidents, to mitigate, to the extent practicable, harmful effects of security incidents known to MIE, or to document such Incidents and their outcomes in accordance with the implementation specifications of the Security Rule, 45 C.F.R. § 164.308(a)(6)(ii).

g. MIE failed to assign a unique name and/or number for identifying and tracking user identity in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(iv).

i. MIE failed to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI, in violation of 45 C.F.R. § 164.312(b).

j. MIE failed to implement procedures to verify that a person or entity seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

k. MIE failed to adhere to the Minimum Necessary Standard when using or disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

47. Plaintiff, Arizona, is entitled to certain statutory damages pursuant to 42 U.S.C. 1320d-5(d)(2).

**Count II**
**Arizona: Violation of Ariz. Rev. Stat. § 44-1522**

48. Plaintiff, Arizona, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

49. The Defendants' conduct constitutes a violation of Ariz. Rev. Stat. § 44-1522.

50. The information security failings outlined in the preceding paragraphs constitute unfair or deceptive acts or practices in violation of Ariz. Rev. Stat. § 44-1522.

51. For example, MIE committed unfair or deceptive acts or practices by representing, in connection with the advertisement and sale of its services, that it maintained appropriate Administrative and Technical Safeguards to protect patients' ePHI and other appropriate measures to protect consumers' sensitive information, when such was not the case.

52. Defendants' security failings were also likely to cause substantial injury to consumers, including identity theft, and such injury was not reasonably avoidable by the consumers themselves, particularly in light of Defendants' failure to notify consumers in the

most expedient manner possible, nor would such injury be outweighed by any countervailing benefits to consumers or competition.

53. Defendants' conduct was also willful, as, among other things, they knew or should have known that their unfair or deceptive acts or practices were unlawful.

54. Plaintiff, Arizona, is entitled to injunctive relief, restitution to all affected persons, and disgorgement of Defendants' profits or revenues obtained by means of its unlawful conduct pursuant to Ariz. Rev. Stat. § 44-1528; civil penalties pursuant to Ariz. Rev. Stat. § 44-1531; and attorney fees and costs pursuant to Ariz. Rev. Stat. § 44-1534.

**Count III**
**Arkansas: Violation of HIPAA Safeguards**

55. Plaintiff, Arkansas, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

56. Defendants' conduct constitutes violations of Administrative Safeguards, Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

a. MIE failed to review and modify security measures needed to continue the provision of reasonable and appropriate protection of ePHI in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.306(e).

b. MIE failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI that it maintained in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

c. MIE failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in accordance with the

implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B).

d. MIE failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and Security Incident tracking reports in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

e. MIE failed to implement policies and procedures that, based upon its access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process that includes ePHI in accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

f. MIE failed to implement policies and procedures to address Security Incidents, including suspected Security Incidents, to mitigate, to the extent practicable, harmful effects of security incidents known to MIE, or to document such Incidents and their outcomes in accordance with the implementation specifications of the Security Rule, 45 C.F.R. § 164.308(a)(6)(ii).

g. MIE failed to assign a unique name and/or number for identifying and tracking user identity in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(iv).

i. MIE failed to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI, in violation of 45 C.F.R. § 164.312(b).

j. MIE failed to implement procedures to verify that a person or entity seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

k. MIE failed to adhere to the Minimum Necessary Standard when using or disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

57. Plaintiff, Arkansas, is entitled to certain statutory damages pursuant to 42 U.S.C. 1320d-5(d)(2).

**Count IV**
**Arkansas: Deceptive Acts in Violation of Ark. § 4-88-101**

58. Plaintiff, Arkansas, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

59. The Defendants' conduct constitutes a violation of Ark. Code § 4-88-108.

60. The information security failings outlined in paragraphs 30 through 40 constitute unfair or deceptive acts in violation of Ark. Code § 4-88-108.

61. MIE committed an unfair or deceptive act by representing that it maintained appropriate Administrative and Technical Safeguards to protect patients' ePHI, and other appropriate measures to protect consumers' sensitive information, when such was not the case, in violation of Ark. Code Ann. § 4-88-107(b) and Ark. Code Ann. § 4-88-108.

62. Plaintiff, Arkansas, is entitled to civil penalties pursuant to Ark. Code § 4-88-113(a)(3), attorney's fees and costs pursuant to Ark. Code § 4-88-113(e), and injunctive relief pursuant to Ark. Code § 4-88-113(a)(1).

**Count V**
**Arkansas: Data Breach Violation of Ark. Code § 4-110-105**

63. Plaintiff, Arkansas, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

64. MIE failed to notify affected individuals or others of the Data Breach as required by Ark. Code § 4-110-105.

65. As alleged in paragraphs 32 and 33, Defendants began notifying affected individuals on July 17, 2015 and did not conclude until December 2015. The effective notice date range after the breach was discovered was between 52 days and six months.

66. By waiting between 52 days and six months to notify affected individuals, Defendants violated Ark. Code § 4-110-105.

67. Plaintiff, Arkansas, is entitled to civil penalties pursuant to Ark. Code §§ 4-110-108, 4-88-113(a)(3), attorney fees and costs pursuant to Ark. Code §§ 4-110-108, 4-88-113(e), and injunctive relief pursuant to Ark. Code §§ 4-110-108, 4-88-113(a)(1).

**Count VI**
**Arkansas: Failure to Implement Reasonable Procedures to Protect Personal Information in Violation of Ark. Code § 4-110-104(b)**

68. Plaintiff, Arkansas, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

69. Defendants failed to implement and maintain reasonable procedures to protect and safeguard the unlawful disclosure of personal information in violation of Ark. Code § 4-110-104(b).

70. The information security failings outlined in paragraphs 30 through 40 constitute unreasonable safeguard procedures in violation of Ark. Code § 4-110-104(b).

71. Plaintiff, Arkansas, is entitled to civil penalties pursuant to Ark. Code §§ 4-110-108, 4-88-113(a)(3), attorney fees and costs pursuant to Ark. Code §§ 4-110-108, 4-88-113(e), and injunctive relief pursuant to Ark. Code §§ 4-110-108, 4-88-113(a)(1).

**Count VII**
**Connecticut: Violation of HIPAA Safeguards**

72. Plaintiff, Connecticut, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

73. Defendants' conduct constitutes violations of Administrative Safeguards, Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

a. MIE failed to review and modify security measures needed to continue the provision of reasonable and appropriate protection of ePHI in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.306(e).

b. MIE failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI that it maintained in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

c. MIE failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B).

d. MIE failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and Security Incident

tracking reports in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

e. MIE failed to implement policies and procedures that, based upon its access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process that includes ePHI in accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

f. MIE failed to implement policies and procedures to address Security Incidents, including suspected Security Incidents, to mitigate, to the extent practicable, harmful effects of security incidents known to MIE, or to document such Incidents and their outcomes in accordance with the implementation specifications of the Security Rule, 45 C.F.R. § 164.308(a)(6)(ii).

g. MIE failed to assign a unique name and/or number for identifying and tracking user identity in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(iv).

i. MIE failed to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI, in violation of 45 C.F.R. § 164.312(b).

j. MIE failed to implement procedures to verify that a person or entity seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

k. MIE failed to adhere to the Minimum Necessary Standard when using or disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

74. Plaintiff, Connecticut, is entitled to certain statutory damages pursuant to 42 U.S.C. 1320d-5(d)(2).

**Count VIII**
**Connecticut: Deceptive Acts in Violation of Conn. Gen. Stat. § 42-110b**

75. Plaintiff, Connecticut, incorporates factual allegations in paragraphs 1 through 44 of this Complaint.

76. The Defendants' conduct constitutes a violation of Conn. Gen. Stat. § 42-110b.

77. The information security failings outlined in paragraphs 30 through 40 constitute unfair or deceptive acts in violation of Conn. Gen. Stat. § 42-110b.

78. MIE committed an unfair or deceptive act by representing that it maintained appropriate Administrative and Technical Safeguards to protect patients' ePHI, and other appropriate measures to protect consumers' sensitive information, when such was not the case, in violation of Conn. Gen. Stat. § 42-110b. That misrepresentation was reasonably interpreted by consumers, affecting their decisions to provide sensitive information to MIE.

79. MIE knew or should have known that its acts and practices alleged herein were unfair and deceptive, and were thus willful violations of Conn. Gen. Stat. §42-110b. MIE is therefore liable for civil penalties of up to $5,000 per willful violation pursuant to General Statutes §42-110o(b).

80. Plaintiff, Connecticut, is entitled to civil penalties pursuant to Conn. Gen. Stat. § 42-110o, attorney fees and costs pursuant to Conn. Gen. Stat. § 42-110m, and injunctive relief pursuant to Conn. Gen. Stat. § 42-110m.

**Count IX**
**Connecticut: Data Breach Violation of Conn. Gen. Stat. § 36a-701b**

81. Plaintiff, Connecticut, incorporates factual allegations in paragraphs 1 through 44 of this Complaint.

82. MIE failed to notify affected individuals or others of the Data Breach as required by Conn. Gen. Stat. § 36a-701b.

83. As alleged in paragraphs 32 and 33, Defendants began notifying affected individuals on July 17, 2015 and did not conclude until December 2015. The effective notice date range after the breach was discovered was between 52 days and six months.

84. By waiting between 52 days and six months to notify affected individuals, Defendants violated Conn. Gen. Stat. § 36a-701b.

85. Pursuant to Conn. Gen. Stat. § 36a-701b(g), a violation of Conn. Gen. Stat. § 36a-701b constitutes an unfair or deceptive trade practice under Conn. Gen. Stat. § 42-110b.

86. MIE knew or should have known that its acts and practices alleged herein were unfair and deceptive, and were thus willful violations of Conn. Gen. Stat. §42-110b. MIE is therefore liable for civil penalties of up to $5,000 per willful violation pursuant to General Statutes §42-110o(b).

87. Plaintiff, Connecticut, is entitled to attorney fees and costs, and injunctive relief pursuant to Conn. Gen. Stat. §§ 36a-701b(g), 42-110m, and injunctive relief pursuant to Conn. Gen. Stat. §§ 36a-701b(g) and 42-110m.

**Count X**
**Connecticut: Failure to Implement Reasonable Procedures to Protect Personal Information in Violation of Conn. Gen. Stat. § 42-471**

88. Plaintiff, Connecticut, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

89. Defendants failed to implement and maintain reasonable procedures to protect and safeguard the unlawful disclosure of personal information in violation of Conn. Gen. Stat. § 42-471.

90. MIE was in possession of Connecticut consumers' "personal information" as that term is defined in Conn. Gen. Stat. § 42-471(c).

91. Defendants failed to implement and maintain reasonable procedures to protect and safeguard personal information in violation of Conn. Gen. Stat. § 42-471.

92. Plaintiff, Connecticut, is entitled to civil penalties pursuant to Conn. Gen. Stat. §§ 42-471(e).

**Count XI**
**Florida: Violation of HIPAA Safeguards**

93. Plaintiff, Florida, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

94. Defendants' conduct constitutes violations of Administrative Safeguards, Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

a. MIE failed to review and modify security measures needed to continue the provision of reasonable and appropriate protection of ePHI in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.306(e).

b. MIE failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI that it maintained in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

c. MIE failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B).

d. MIE failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and Security Incident tracking reports in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

e. MIE failed to implement policies and procedures that, based upon its access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process that includes ePHI in accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

f. MIE failed to implement policies and procedures to address Security Incidents, including suspected Security Incidents, to mitigate, to the extent practicable, harmful effects of security incidents known to MIE, or to document such Incidents and their outcomes in accordance with the implementation specifications of the Security Rule, 45 C.F.R. § 164.308(a)(6)(ii).

g. MIE failed to assign a unique name and/or number for identifying and tracking user identity in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(iv).

i. MIE failed to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI, in violation of 45 C.F.R. § 164.312(b).

j. MIE failed to implement procedures to verify that a person or entity seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

k. MIE failed to adhere to the Minimum Necessary Standard when using or disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

95. Plaintiff, Florida, is entitled to certain statutory damages pursuant to 42 U.S.C. 1320d-5(d)(2).

**Count XII**
**Florida: Deceptive Acts in Violation of Section 501.204, Florida Statutes**

96. Plaintiff, Florida, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

97. The Defendants' conduct constitutes a violation of Section 501.204, Florida Statutes.

98. The information security failings outlined in paragraphs 34 through 44 constitute unfair or deceptive acts in violation of Section 501.204, Florida Statutes.

99. MIE committed an unfair or deceptive act by representing that it maintained appropriate Administrative and Technical Safeguards to protect patients' ePHI, and other appropriate measures to protect consumers' sensitive information, when such was not the case, in violation of Section 501.204, Florida Statutes.

100. Plaintiff, Florida, is entitled to civil penalties pursuant to Section 501.2075, Florida Statutes, attorney fees and costs pursuant to Section 501.2105, Florida Statutes, and injunctive relief pursuant to Section 501.207(b), Florida Statutes.

**Count XIII**
**Florida: Data Breach Violation of Section 501.171, Florida Statutes**

101. Plaintiff, Florida, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

102. MIE failed to notify affected individuals or others of the Data Breach as required by Section 501.171(4), Florida Statutes.

103. As alleged in paragraphs 32 and 33, Defendants began notifying affected individuals on July 17, 2015 and did not conclude until December 2015. The effective notice date range after the breach was discovered was between 52 days and six months.

104. By waiting between 52 days and six months to notify affected individuals, Defendants violated Section 501.171(4), Florida Statutes.

105. Plaintiff, Florida, is entitled to civil penalties pursuant to Section 501.171(9), Florida Statutes, attorney fees and costs pursuant to Section 501.171(9), Florida Statutes and injunctive relief pursuant to Section 501.171(9), Florida Statutes.

**Count XIV**
**Florida: Failure to Implement Reasonable Procedures to Protect Personal Information in Violation of Section 501.171(2), Florida Statutes**

106. Plaintiff, Florida, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

107. Defendants failed to implement and maintain reasonable procedures to protect and safeguard the unlawful disclosure of personal information in violation of Section 501.171(2), Florida Statutes.

108. The information security failings outlined in paragraphs 34 through 44 constitute unreasonable safeguard procedures in violation of Section 501.171(2), Florida Statutes.

109. Plaintiff, Florida, is entitled to attorney fees and costs pursuant to Section 501.171(9), Florida Statutes and injunctive relief pursuant to Section 501.171(9), Florida Statutes.

**Count XV**
**Indiana: Violation of HIPAA Safeguards**

110. Plaintiff, Indiana, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

111. Defendants' conduct constitutes violations of Administrative Safeguards, Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

a. MIE failed to review and modify security measures needed to continue the provision of reasonable and appropriate protection of ePHI in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.306(e).

b. MIE failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI that it maintained in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

c. MIE failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B).

d. MIE failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and Security Incident

tracking reports in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

e. MIE failed to implement policies and procedures that, based upon its access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process that includes ePHI in accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

f. MIE failed to implement policies and procedures to address Security Incidents, including suspected Security Incidents, to mitigate, to the extent practicable, harmful effects of security incidents known to MIE, or to document such Incidents and their outcomes in accordance with the implementation specifications of the Security Rule, 45 C.F.R. § 164.308(a)(6)(ii).

g. MIE failed to assign a unique name and/or number for identifying and tracking user identity in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(iv).

i. MIE failed to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI, in violation of 45 C.F.R. § 164.312(b).

j. MIE failed to implement procedures to verify that a person or entity seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

k. MIE failed to adhere to the Minimum Necessary Standard when using or disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

112. Plaintiff, Indiana, is entitled to certain statutory damages pursuant to 42 U.S.C. 1320d-5(d)(2).

**Count XVI**
**Indiana: Deceptive Acts in Violation of Ind. Code § 24-5-0.5-3**

113. Plaintiff, Indiana, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

114. The Defendants' conduct constitutes a violation of Ind. Code § 24-5-0.5-3.

115. The information security failings outlined in paragraphs 30 through 40 constitute unfair or deceptive acts in violation of Ind. Code § 24-5-0.5-3.

116. MIE committed an unfair or deceptive act by representing that it maintained appropriate Administrative and Technical Safeguards to protect patients' ePHI, and other appropriate measures to protect consumers' sensitive information, when such was not the case, in violation of Ind. Code § 24-5-0.5-3.

117. Plaintiff, Indiana, is entitled to civil penalties pursuant to Ind. Code § 24-5-0.5-4(g), attorney fees and costs pursuant to Ind. Code § 24-5-0.5-4(c), and injunctive relief pursuant to Ind. Code § 24-5-0.5-4(c).

**Count XVII**
**Indiana: Failure to Implement Reasonable Procedures to Protect Personal Information in Violation of Ind. Code § 24-4.9-3-3.5**

118. Plaintiff, Indiana, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

119. Defendants failed to implement and maintain reasonable procedures to protect and safeguard the unlawful disclosure of personal information in violation of Ind. Code § 24-4.9-3-3.5(c).

120. The information security failings outlined in paragraphs 30 through 444 constitute unreasonable safeguard procedures in violation of Ind. Code § 24-5-0.5-3.5.

121. Defendants are not exempt from Ind. Code § 24-5-0.5-3.5, as the Defendants did not comply with a HIPAA compliancy plan. Ind. Code § 24-5-0.5-3.5(a)(6).

122. Plaintiff, Indiana, is entitled to civil penalties pursuant to Ind. Code § 24-4.9-3-3.5(f)(2), attorney fees and costs pursuant to Ind. Code § 24-4.9-3-3.5(f)(3), and injunctive relief pursuant to Ind. Code § 24-4.9-3-3.5(f)(1).

**Count XVIII**
**Iowa: Violation of HIPAA Safeguards**

123. Plaintiff, Iowa, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

124. Defendants' conduct constitutes violations of Administrative Safeguards, Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

a. MIE failed to review and modify security measures needed to continue the provision of reasonable and appropriate protection of ePHI in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.306(e).

b. MIE failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI that it maintained in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

c. MIE failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B).

d. MIE failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and Security Incident tracking reports in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

e. MIE failed to implement policies and procedures that, based upon its access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process that includes ePHI in accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

f. MIE failed to implement policies and procedures to address Security Incidents, including suspected Security Incidents, to mitigate, to the extent practicable, harmful effects of security incidents known to MIE, or to document such Incidents and their outcomes in accordance with the implementation specifications of the Security Rule, 45 C.F.R. § 164.308(a)(6)(ii).

g. MIE failed to assign a unique name and/or number for identifying and tracking user identity in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(iv).

i. MIE failed to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI, in violation of 45 C.F.R. § 164.312(b).

j. MIE failed to implement procedures to verify that a person or entity seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

k. MIE failed to adhere to the Minimum Necessary Standard when using or disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

125. Plaintiff, Iowa, is entitled to certain statutory damages pursuant to 42 U.S.C. 1320d-5(d)(2).

**Count XIX**
**Iowa: Deceptive Acts in Violation of Iowa Code § 714.16**

126. Plaintiff, Iowa, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

127. The Defendants' conduct constitutes a violation of Iowa Code § 714.16.

128. The information security failings outlined in paragraphs 30 through 40 constitute unfair or deceptive acts in violation of Iowa Code § 714.16.

129. MIE committed an unfair or deceptive act by representing that it maintained appropriate Administrative and Technical Safeguards to protect patients' ePHI, and other appropriate measures to protect consumers' sensitive information, when such was not the case, in violation of Iowa Code § 714.16.

130. Plaintiff, Iowa, is entitled to civil penalties pursuant to Iowa Code § 714.16(8), attorney fees and costs pursuant to Iowa Code § 714.16(11), and injunctive relief pursuant to Iowa Code § 714.16(7).

**Count XX**
**Iowa: Data Breach Violation of Iowa Code § 715C.2**

131. Plaintiff, Iowa, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

132. MIE failed to notify affected individuals or others of the Data Breach as required by Iowa Code § 715C.2.

133. As alleged in paragraphs 32 and 33, Defendants began notifying affected individuals on July 17, 2015 and did not conclude until December 2015. The effective notice date range after the breach was discovered was between 52 days and six months.

134. By waiting between 52 days and six months to notify affected individuals, Defendants violated Iowa Code § 715C.2.

135. Plaintiff, Iowa, is entitled to civil penalties pursuant to Iowa Code §§ 715C.2(9), 714.16(7), attorney fees and costs pursuant to Iowa Code §§ 715C.2(9), 714.16(7), and injunctive relief pursuant to Iowa Code §§ 715C.2(9), 714.16(7).

**Count XXI**
**Kansas: Violation of HIPAA Safeguards**

136. Plaintiff, Kansas, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

137. Defendants' conduct constitutes violations of Administrative Safeguards, Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

a. MIE failed to review and modify security measures needed to continue the provision of reasonable and appropriate protection of ePHI in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.306(e).

b. MIE failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI that it maintained in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

c. MIE failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B).

d. MIE failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and Security Incident tracking reports in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

e. MIE failed to implement policies and procedures that, based upon its access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process that includes ePHI in accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

f. MIE failed to implement policies and procedures to address Security Incidents, including suspected Security Incidents, to mitigate, to the extent practicable, harmful effects of security incidents known to MIE, or to document such Incidents and their outcomes in accordance with the implementation specifications of the Security Rule, 45 C.F.R. § 164.308(a)(6)(ii).

g. MIE failed to assign a unique name and/or number for identifying and tracking user identity in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(iv).

i. MIE failed to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI, in violation of 45 C.F.R. § 164.312(b).

j. MIE failed to implement procedures to verify that a person or entity seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

k. MIE failed to adhere to the Minimum Necessary Standard when using or disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

138. Plaintiff, Kansas, is entitled to certain statutory damages pursuant to 42 U.S.C. 1320d-5(d)(2).

**Count XXII**
**Kansas: Deceptive Acts in Violation of Kan. Stat. § 50-626**

139. Plaintiff, Kansas, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

140. The Defendants' conduct constitutes a violation of Kan. Stat. § 50-626**.**

141. The information security failings outlined in paragraphs 34 through 43 constitute unfair or deceptive acts in violation of Kan. Stat. § 50-626.

142. MIE committed an unfair or deceptive act by representing that it maintained appropriate Administrative and Technical Safeguards to protect patients' ePHI, and other

appropriate measures to protect consumers' sensitive information, when such was not the case, in violation of Kan. Stat. § 50-626.

143. Plaintiff, Kansas, is entitled to civil penalties pursuant to Kan. Stat. § 50-636, attorney fees and costs pursuant to Kan. Stat. § 50-632(a)(4), and injunctive relief pursuant to Kan. Stat. § 50-632(a)(2).

**Count XXIII**
**Kansas: Data Breach Violation of Kan. Stat. § 50-7a02**

144. Plaintiff, Kansas, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

145. MIE failed to notify affected individuals or others of the Data Breach as required by Kan. Stat. § 50-7a02.

146. As alleged in paragraphs 32 and 33, Defendants began notifying affected individuals on July 17, 2015 and did not conclude until December 2015. The effective notice date range after the breach was discovered was between 52 days and six months.

147. By waiting between 52 days and six months to notify affected individuals, Defendants violated Kan. Stat. § 50-7a02.

148. Plaintiff, Kansas, is entitled to appropriate relief pursuant Kan. Stat. § 50-7a02(g).

**Count XXIV**
**Kansas: Failure to Implement Reasonable Procedures to Protect Personal Information in Violation of Kan. Stat. § 50-6139b(b)(1)**

149. Plaintiff, Kansas, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

150. Defendants failed to implement and maintain reasonable procedures to protect and safeguard the unlawful disclosure of personal information in violation of Kan. Stat. § 50-6139b(b)(1).

151. The information security failings outlined in paragraphs 34 through 43 constitute unreasonable safeguard procedures in violation of Kan. Stat. § 50-6139b(b)(1).

152. Plaintiff, Kansas, is entitled to civil penalties pursuant to Kan. Stat. §§ 50-6139b(d, e), 50-636, attorney fees and costs pursuant to Kan. Stat. §§ 50-6139b(d, e), 50-636(c), and injunctive relief pursuant to Kan. Stat. §§ 50-6139b(d, e), 50-632(a)(2).

**Count XXV**
**Kentucky: Violation of HIPAA Safeguards**

153. Plaintiff, Kentucky, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

154. Defendants' conduct constitutes violations of Administrative Safeguards, Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

a. MIE failed to review and modify security measures needed to continue the provision of reasonable and appropriate protection of ePHI in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.306(e).

b. MIE failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI that it maintained in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

c. MIE failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B).

d. MIE failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and Security Incident tracking reports in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

e. MIE failed to implement policies and procedures that, based upon its access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process that includes ePHI in accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

f. MIE failed to implement policies and procedures to address Security Incidents, including suspected Security Incidents, to mitigate, to the extent practicable, harmful effects of security incidents known to MIE, or to document such Incidents and their outcomes in accordance with the implementation specifications of the Security Rule, 45 C.F.R. § 164.308(a)(6)(ii).

g. MIE failed to assign a unique name and/or number for identifying and tracking user identity in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(iv).

i. MIE failed to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI, in violation of 45 C.F.R. § 164.312(b).

j. MIE failed to implement procedures to verify that a person or entity seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

k. MIE failed to adhere to the Minimum Necessary Standard when using or disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

155. Plaintiff, Kentucky, is entitled to certain statutory damages pursuant to 42 U.S.C. 1320d-5(d)(2).

**Count XXVI**
**Kentucky: Deceptive Acts in Violation of Ky. Rev. Stat. § 367.170**

156. Plaintiff, Kentucky, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

157. The Defendants' conduct constitutes a violation of Ky. Rev. Stat. § 367.170.

158. The information security failings outlined in paragraphs 23 through 44 constitute unfair or deceptive acts in violation of Ky. Rev. Stat. § 367.170.

159. MIE committed an unfair or deceptive act by representing that it maintained appropriate Administrative and Technical Safeguards to protect patients' ePHI, and other appropriate measures to protect consumers' sensitive information, when such was not the case, in violation of Ky. Rev. Stat. § 367.170.

160. Plaintiff, Kentucky, is entitled to civil penalties pursuant to Ky. Rev. Stat. § 367.990(2), and injunctive relief pursuant to Ky. Rev. Stat. § 367.190.

**Count XXVII**
**Louisiana: Violation of HIPAA Safeguards**

161. Plaintiff, Louisiana, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

162. Defendants' conduct constitutes violations of Administrative Safeguards, Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

a. MIE failed to review and modify security measures needed to continue the provision of reasonable and appropriate protection of ePHI in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.306(e).

b. MIE failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI that it maintained in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

c. MIE failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B).

d. MIE failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and Security Incident tracking reports in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

e. MIE failed to implement policies and procedures that, based upon its access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process that includes ePHI in accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

f. MIE failed to implement policies and procedures to address Security Incidents, including suspected Security Incidents, to mitigate, to the extent practicable, harmful effects of security incidents known to MIE, or to document such Incidents and their outcomes in accordance with the implementation specifications of the Security Rule, 45 C.F.R. § 164.308(a)(6)(ii).

g. MIE failed to assign a unique name and/or number for identifying and tracking user identity in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(iv).

i. MIE failed to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI, in violation of 45 C.F.R. § 164.312(b).

j. MIE failed to implement procedures to verify that a person or entity seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

k. MIE failed to adhere to the Minimum Necessary Standard when using or disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

163. Plaintiff, Louisiana, is entitled to certain statutory damages pursuant to 42 U.S.C. 1320d-5(d)(2).

**Count XXVIII**
**Louisiana: Deceptive Acts in Violation of La. Rev. Stat. § 51:1405**

164. Plaintiff, Louisiana, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

165. The Defendants' conduct constitutes a violation of La. Rev. Stat. § 51:1405.

166. The information security failings outlined in paragraphs 30 through 40 constitute unfair or deceptive acts in violation of La. Rev. Stat. § 51:1405.

167. MIE committed an unfair or deceptive act by representing that it maintained appropriate Administrative and Technical Safeguards to protect patients' ePHI, and other appropriate measures to protect consumers' sensitive information, when such was not the case, in violation of La. Rev. Stat. § 51:1405.

168. Plaintiff, Louisiana, is entitled to civil penalties pursuant and injunctive relief pursuant to La. Rev. Stat. § 51:1407.

**Count XXIX**
**Louisiana: Data Breach Violation of La. Rev. Stat. § 51:3074**

169. Plaintiff, Louisiana, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

170. MIE failed to notify affected individuals or others of the Data Breach as required by La. Rev. Stat. § 51:3074.

171. As alleged in paragraphs 32 and 33, Defendants began notifying affected individuals on July 17, 2015 and did not conclude until December 2015. The effective notice date range after the breach was discovered was between 52 days and six months.

172. By waiting between 52 days and six months to notify affected individuals, Defendants violated La. Rev. Stat. § 51:3074.

173. Plaintiff, Louisiana, is entitled to damages and civil penalties pursuant to La. Rev. Stat. 51:3075 and 16 La. Admin. Code Pt III, 701.

**Count XXX**
**Michigan: Violation of HIPAA Safeguards**

174. Plaintiff, Michigan, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

175. Defendants' conduct constitutes violations of Administrative Safeguards, Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

a. MIE failed to review and modify security measures needed to continue the provision of reasonable and appropriate protection of ePHI in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.306(e).

b. MIE failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI that it maintained in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

c. MIE failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B).

d. MIE failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and Security Incident tracking reports in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

e. MIE failed to implement policies and procedures that, based upon its access authorization policies, establish, document, review, and modify a user's right of

access to a workstation, transaction, program, or process that includes ePHI in accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

f. MIE failed to implement policies and procedures to address Security Incidents, including suspected Security Incidents, to mitigate, to the extent practicable, harmful effects of security incidents known to MIE, or to document such Incidents and their outcomes in accordance with the implementation specifications of the Security Rule, 45 C.F.R. § 164.308(a)(6)(ii).

g. MIE failed to assign a unique name and/or number for identifying and tracking user identity in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(iv).

i. MIE failed to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI, in violation of 45 C.F.R. § 164.312(b).

j. MIE failed to implement procedures to verify that a person or entity seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

k. MIE failed to adhere to the Minimum Necessary Standard when using or disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

176. Plaintiff, Michigan, is entitled to certain statutory damages pursuant to 42 U.S.C. 1320d-5(d)(2).

**Count XXXI**
**Michigan: Deceptive Acts in Violation of Mich. Comp. Laws § 445.901**

177. Plaintiff, Michigan, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

178. The Defendants' conduct constitutes a violation of Mich. Comp. Laws § 445.901.

179. The information security failings outlined in paragraphs 30 through 43 constitute unfair or deceptive acts in violation of Mich. Comp. Laws § 445.901.

180. MIE committed an unfair or deceptive act by representing that it maintained appropriate Administrative and Technical Safeguards to protect patients' ePHI, and other appropriate measures to protect consumers' sensitive information, when such was not the case, in violation of Mich. Comp. Laws § 445.901.

181. Plaintiff, Michigan, is entitled to civil penalties pursuant to Mich. Comp. Laws § 445.905, and injunctive relief pursuant to Mich. Comp. Laws § 445.905.

**Count XXXII**
**Michigan: Data Breach Violation of Mich. Comp. Laws § 445.72**

182. Plaintiff, Michigan, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

183. MIE failed to notify affected individuals or others of the Data Breach as required by Mich. Comp. Laws § 445.72.

184. As alleged in paragraphs 32 and 33, Defendants began notifying affected individuals on July 17, 2015 and did not conclude until December 2015. The effective notice date range after the breach was discovered was between 52 days and six months.

185. By waiting between 52 days and six months to notify affected individuals, Defendants violated Mich. Comp. Laws § 445.72.

186. Plaintiff, Michigan, is entitled to civil penalties pursuant to Mich. Comp. Laws § 445.72(13).

**Count XXXIII**
**Minnesota: Violation of HIPAA Safeguards**

187. Plaintiff, Minnesota, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

188. Defendants' conduct constitutes violations of Administrative Safeguards, Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

a. MIE failed to review and modify security measures needed to continue the provision of reasonable and appropriate protection of ePHI in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.306(e).

b. MIE failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI that it maintained in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

c. MIE failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B).

d. MIE failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and Security Incident tracking reports in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

e. MIE failed to implement policies and procedures that, based upon its access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process that includes ePHI in accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

f. MIE failed to implement policies and procedures to address Security Incidents, including suspected Security Incidents, to mitigate, to the extent practicable, harmful effects of security incidents known to MIE, or to document such Incidents and their outcomes in accordance with the implementation specifications of the Security Rule, 45 C.F.R. § 164.308(a)(6)(ii).

g. MIE failed to assign a unique name and/or number for identifying and tracking user identity in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(iv).

i. MIE failed to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI, in violation of 45 C.F.R. § 164.312(b).

j. MIE failed to implement procedures to verify that a person or entity seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

k. MIE failed to adhere to the Minimum Necessary Standard when using or disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

189. Plaintiff, Minnesota, is entitled to certain statutory damages pursuant to 42 U.S.C. 1320d-5(d)(2).

**Count XXXIV**
**Minnesota: Deceptive Acts in Violation of Minn. Stat. § 325F.69**

190. Plaintiff, Minnesota, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

191. Minnesota Statutes section 325F.69, subdivision 1 reads:

> The act, use, or employment by any person of any fraud, false pretense, false promise, misrepresentation, misleading statement or deceptive practice, with the intent that others rely thereon in connection with the sale of any merchandise, whether or not any person has in fact been misled, deceived, or damaged thereby, is enjoinable as provided in section 325F.70

Minn. Stat. § 325F.69, subd. 1 (2017).

192. The term "merchandise" within the meaning of Minnesota Statutes section 325F.69 includes services. *See* Minn. Stat. § 325F.68, subd. 2 (2017).

193. Defendants have repeatedly violated Minnesota Statutes section 325F.69, subdivision 1, by engaging in the deceptive and fraudulent practices described in this Complaint. For example, Defendants falsely represented to Minnesota persons that Defendants would protect and safeguard their protected health information and sensitive personal information—including, but not limited to, by using encryption tools and maintaining appropriate Administrative and Technical Safeguards to protect Minnesota persons' ePHI, as well as other appropriate measures to protect Minnesota persons' sensitive personal information—when such was not the case, resulting in the exposure of Minnesota persons' protected health information and sensitive personal information as described in this Complaint.

194. As a result of the practices described in this Complaint, hackers accessed and exfiltrated the protected health information of more than 8,000 Minnesotans (including more than 5,000 Minnesotans who also had their Social Security numbers exposed as well). The protected health information and sensitive personal information that was hacked includes an individual's name, telephone number, mailing address, username, hashed password, security question and answer, spousal information (including name and date of birth), email address, date of birth, Social Security number, lab results, health insurance policy information, diagnosis, disability code, doctor's name, medical conditions, and child's name and birth statistics. These Minnesota persons had their protected health information and personal information exposed in connection with their seeking treatment from healthcare providers, physician practices, hospitals, and/or other organizations which are or were located and/or operated within Minnesota.

195. Special circumstances exist that triggered a duty on the part of Defendants to disclose material facts related to vulnerabilities within Defendants' computer systems to Minnesota persons. First, Defendants had special knowledge of the vulnerabilities in Defendants' computers systems, and that hackers had exposed these vulnerabilities, leading to the release of Minnesotans protected health information and personal information. Minnesotans did not have knowledge of these vulnerabilities or the release of this information at the time of their treatment. Minnesotans lack of knowledge was also caused, in part, by Defendants failure to timely notify Minnesotans of the security breach of Defendants' computer systems. Second, Defendants did not say enough to prevent the representations it made to Minnesotans from being deceptive and misleading.

196. Defendants knew or had reason to know that Minnesotans would place their trust in Defendants and rely on Defendants to inform them of material facts relating to the

vulnerabilities in Defendants' computers systems, and that hackers had exposed these vulnerabilities. Defendants abused that trust by making misrepresentations, or concealing material facts, about these vulnerabilities.

197. Given the representations it made, its special knowledge, and the circumstances described in this Complaint, Defendants had a duty to disclose material facts to Minnesota persons in connection with the data breach described in this Complaint. By not doing so, Defendants failed to disclose material information in violation of Minnesota Statutes section 325F.69, subdivision 1.

198. Due to the deceptive and fraudulent conduct described in this Complaint, Minnesota persons made payments to Defendants for goods and services that they otherwise would not have purchased or in amounts that they should not have been required to pay.

199. Defendants' conduct, practices, actions, and material omissions described in this Complaint constitute multiple, separate violations of Minnesota Statutes section 325F.69.

200. Plaintiff, Minnesota, is entitled to civil penalties pursuant to Minn. Stat. § 8.31; attorney fees and costs pursuant to Minn. Stat. § 8.31; injunctive relief pursuant to Minn. Stat. § 8.31 and § 325F.70; restitution under the *parens patriae* doctrine, the general equitable powers of this Court, and§ 8.31; and any such further relief as provided by law or equity, or as the Court deems appropriate and just.

**Count XXXV**
**Minnesota: Deceptive Acts in Violation of Minn. Stat. § 325D.44**

201. Plaintiff, Minnesota, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

202. Minnesota Statutes section 325D.44, subdivision 1 provides in part that:

> A person engages in a deceptive trade practice when, in the course of business, vocation, or occupation, the person:
> ***
> (5) represents that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have or that a person has a sponsorship, approval, status, affiliation or connection that the person does not have;
> ***
> (7) represents that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another;
> *** or
> (13) engages in any other conduct which similarly creates a likelihood of confusion or of misunderstanding.

Minn. Stat. § 325D.44, subd. 1 (2017).

203. Defendants have repeatedly violated Minnesota Statutes section 325D.44, subdivision 1, by engaging in the deceptive and fraudulent conduct described in this Complaint, including by making false, deceptive, fraudulent, and/or misleading representations and material omissions to Minnesota persons regarding their products and services. These misrepresentations and material omissions include but are not limited to: (1) by making misrepresentations about protecting Minnesota persons ePHI and sensitive personal information, Defendants represented that their products and/or services had characteristics that they did not have in violation of Minn. Stat. § 325D.44, subd. 1(5), and were of a particular standard, quality, or grade, when they were of another in violation of Minn. Stat. § 325D.44, subd. 1(7); and (2) by falsely representing to Minnesota persons that Defendants would protect and safeguard their protected health information and sensitive personal information—including, but not limited to, by using encryption tools and maintaining appropriate Administrative and Technical Safeguards to protect Minnesota persons' ePHI, as well as other appropriate measures to protect Minnesota persons' sensitive personal information—when such was not the case, resulting in the exposure of Minnesota persons' protected health information and sensitive personal information as described

in this Complaint, Defendant engaged in conduct that creates a likelihood of confusing or of misunderstanding in violation of Minn. Stat. § 325D.44, subd. 1(13).

204. As a result of the practices described in this Complaint, hackers accessed and exfiltrated the protected health information of more than 8,000 Minnesotans (including more than 5,000 Minnesotans who also had their Social Security numbers exposed as well). The protected health information and sensitive personal information that was hacked includes an individual's name, telephone number, mailing address, username, hashed password, security question and answer, spousal information (including name and date of birth), email address, date of birth, Social Security number, lab results, health insurance policy information, diagnosis, disability code, doctor's name, medical conditions, and child's name and birth statistics. These Minnesota persons had their protected health information and personal information exposed as a result of their seeking treatment from healthcare providers, physician practices, hospitals, and/or other organizations which are or were located and/or operated within Minnesota.

205. Special circumstances exist that triggered a duty on the part of Defendants to disclose material facts related to vulnerabilities within Defendants' computer systems to Minnesota persons. First, Defendants had special knowledge of the vulnerabilities in Defendants' computers systems, and that hackers had exposed these vulnerabilities, leading to the release of Minnesotans protected health information and personal information. Minnesota did not have knowledge of these vulnerabilities or the release of this information at the time of their treatment. Minnesotans lack of knowledge was also caused, in part, by Defendants failure to timely notify Minnesotans of the security breach of Defendants' computer systems. Second, Defendants did not say enough to prevent the representations it made to Minnesotans from being deceptive and misleading.

206. Defendants knew or had reason to know that Minnesotans would place their trust in Defendants and rely on Defendants to inform them of material facts relating to the vulnerabilities in Defendants' computers systems, and that hackers had exposed these vulnerabilities. Defendants abused that trust by making misrepresentations, or concealing material facts, about these vulnerabilities.

207. Given the representations it made, its special knowledge, and the circumstances described in this Complaint, Defendants had a duty to disclose material facts to Minnesota persons in connection with the data breach described in this Complaint. By not doing so, Defendants failed to disclose material information in violation of Minnesota Statutes section 325F.69, subdivision 1.

208. Due to the deceptive and fraudulent conduct described in this Complaint, Minnesota persons made payments to Defendants for goods and services that they otherwise would not have purchased or in amounts that they should not have been required to pay.

209. Defendants' conduct, practices, and actions described in this Complaint constitute multiple, separate violations of Minnesota Statutes section 325D.44.

210. Plaintiff, Minnesota, is entitled to civil penalties pursuant to Minn. Stat. § 8.31; attorney fees and costs pursuant to Minn. Stat. § 8.31; injunctive relief pursuant to Minn. Stat. § 8.31 and § 325D.45; restitution under the *parens patriae* doctrine, the general equitable powers of this Court, and§ 8.31; and any such further relief as provided by law or equity, or as the Court deems appropriate and just.

**Count XXXVI**
**Minnesota: Data Breach Violation of Minn. Stat. § 325E.61**

211. Plaintiff, Minnesota, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

212. MIE failed to notify affected individuals or others of the Data Breach as required by Minn. Stat. § 325E.61.

213. As alleged in paragraphs 32 and 33, Defendants began notifying affected individuals on July 17, 2015 and did not conclude until December 2015. The effective notice date range after the breach was discovered was between 52 days and six months.

214. By waiting between 52 days and six months to notify affected individuals, Defendants violated Minn. Stat. § 325E.61.

215. Minnesota Statutes 325E.61, subdivision 1(a) provides in part that:

> Any person or business that conducts business in this state, and that owns or licenses data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay.

Minn. Stat. § 325E.61, subd. 1(a) (2017).

216. At all relevant times, Defendants conducted business in Minnesota and owned or licensed data that included personal information.

217. Defendants have violated Minnesota Statutes section 325E.61, subdivision 1(a) by failing to, without unreasonable delay, expediently notify Minnesota victims of the data breach described in this Complaint. Despite knowing that it exposed the personal information, including persons' names and Social Security numbers, of Minnesota persons, Defendants unreasonably delayed providing notice of this breach to Minnesota residents.

218. Defendants' conduct, practices, and actions described in this Complaint constitute multiple, separate violations of Minnesota Statutes section 325E.61.

219. Plaintiff, Minnesota, is entitled to civil penalties pursuant to Minn. Stat. § 8.31 and § 325E.61, subd. 6; attorney fees and costs pursuant to Minn. Stat. § 8.31 and § 325E.61; subd. 6; injunctive relief pursuant to Minn. Stat. § 8.31 and § 325E.61, subd. 6; restitution under the *parens patriae* doctrine, the general equitable powers of this Court, and Minn. Stat. § 8.31; and any such further relief as provided by law or equity, or as the Court deems appropriate and just.

**Count XXXVII**
**Nebraska: Violation of HIPAA Safeguards**

220. Plaintiff, Nebraska, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

221. Defendants' conduct constitutes violations of Administrative Safeguards, Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

a. MIE failed to review and modify security measures needed to continue the provision of reasonable and appropriate protection of ePHI in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.306(e).

b. MIE failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI that it maintained in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

c. MIE failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B).

d. MIE failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and Security Incident tracking reports in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

e. MIE failed to implement policies and procedures that, based upon its access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process that includes ePHI in accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

f. MIE failed to implement policies and procedures to address Security Incidents, including suspected Security Incidents, to mitigate, to the extent practicable, harmful effects of security incidents known to MIE, or to document such Incidents and their outcomes in accordance with the implementation specifications of the Security Rule, 45 C.F.R. § 164.308(a)(6)(ii).

g. MIE failed to assign a unique name and/or number for identifying and tracking user identity in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(iv).

i. MIE failed to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI, in violation of 45 C.F.R. § 164.312(b).

j. MIE failed to implement procedures to verify that a person or entity seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

k. MIE failed to adhere to the Minimum Necessary Standard when using or disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

222. Plaintiff, Nebraska, is entitled to certain statutory damages pursuant to 42 U.S.C. 1320d-5(d)(2).

**Count XXXVIII**
**Nebraska: Deceptive Acts in Violation of Neb. Rev. Stat. § 59-1602**

223. Plaintiff, Nebraska, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

224. The Defendants' conduct constitutes a violation of Neb. Rev. Stat. § 59-1602.

225. The information security failings outlined in paragraphs 34 through 44 constitute unfair or deceptive acts in violation of Neb. Rev. Stat. § 59-1602.

226. MIE committed an unfair or deceptive act by representing that it maintained appropriate Administrative and Technical Safeguards to protect patients' ePHI, and other appropriate measures to protect consumers' sensitive information, when such was not the case, in violation of Neb. Rev. Stat. § 59-1602.

227. Plaintiff, Nebraska, is entitled to civil penalties pursuant to Neb. Rev. Stat. § 59-1614, attorney fees and costs pursuant to Neb. Rev. Stat. § 59-1602(1), and injunctive relief pursuant to Neb. Rev. Stat. § 59-1608.

**Count XXXIX**
**Nebraska: Data Breach Violation of Neb. Rev. Stat. § 87-803**

228. Plaintiff, Nebraska, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

229. MIE failed to notify affected individuals or others of the Data Breach as required by Neb. Rev. Stat. § 87-803.

230. As alleged in paragraphs 32 and 33, Defendants began notifying affected individuals on July 17, 2015 and did not conclude until December 2015. The effective notice date range after the breach was discovered was between 52 days and six months.

231. By waiting between 52 days and six months to notify affected individuals, Defendants violated Neb. Rev. Stat. § 87-803.

232. Plaintiff, Nebraska, is entitled to direct economic damages for each affected Nebraska resident pursuant to Neb. Rev. Stat. § 87-806.

**Count XL**
**Nebraska: Deceptive Acts in Violation of Neb. Rev. Stat. § 87-302**

233. Plaintiff, Nebraska, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

234. Pursuant to Neb. Rev. Stat. § 87-302(a)(5) and (8), a person engages in a deceptive trade practice when he or she:

> (5) Represents that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have or that a person has a sponsorship, approval, status, affiliation, or connection that he or she does not have; *** or
> (8) Represents that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another;

235. The information security failings outlined in paragraphs 34 through 44 constitute deceptive acts in violation of Neb. Rev. Stat. § 87-302(a)(5) and (8).

236. MIE committed a deceptive act by representing that it maintained appropriate Administrative and Technical Safeguards to protect patients' ePHI, and other appropriate

measures to protect consumers' sensitive information, when such was not the case, in violation of Neb. Rev. Stat. § 87-302(a)(5) and (8).

237. Plaintiff, Nebraska, is entitled to civil penalties pursuant to Neb. Rev. Stat. § 87-303.11, attorney fees and costs pursuant to Neb. Rev. Stat. § 87-303(b), and injunctive relief pursuant to Neb. Rev. Stat. § 87-303.05(1).

**Count XLI**
**North Carolina: Violation of HIPAA Safeguards**

238. Plaintiff, North Carolina, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

239. Defendants' conduct constitutes violations of Administrative Safeguards, Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

a. MIE failed to review and modify security measures needed to continue the provision of reasonable and appropriate protection of ePHI in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.306(e).

b. MIE failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI that it maintained in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

c. MIE failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in accordance with the

implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B).

d. MIE failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and Security Incident tracking reports in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

e. MIE failed to implement policies and procedures that, based upon its access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process that includes ePHI in accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

f. MIE failed to implement policies and procedures to address Security Incidents, including suspected Security Incidents, to mitigate, to the extent practicable, harmful effects of security incidents known to MIE, or to document such Incidents and their outcomes in accordance with the implementation specifications of the Security Rule, 45 C.F.R. § 164.308(a)(6)(ii).

g. MIE failed to assign a unique name and/or number for identifying and tracking user identity in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(iv).

i. MIE failed to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI, in violation of 45 C.F.R. § 164.312(b).

j. MIE failed to implement procedures to verify that a person or entity seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

k. MIE failed to adhere to the Minimum Necessary Standard when using or disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

240. Plaintiff, North Carolina, is entitled to certain statutory damages pursuant to 42 U.S.C. 1320d-5(d)(2).

**Count XLII**
**North Carolina: Deceptive Acts in Violation of N.C. Gen. Stat. § 75-1.1**

241. Plaintiff, North Carolina, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

242. The Defendants' conduct constitutes a violation of N.C. Gen. Stat. § 75-1.1.

243. The information security failings outlined in paragraphs 30 through 40 constitute unfair or deceptive acts in violation of N.C. Gen. Stat. § 75-1.1.

244. MIE committed an unfair or deceptive act by representing that it maintained appropriate Administrative and Technical Safeguards to protect patients' ePHI, and other appropriate measures to protect consumers' sensitive information, when such was not the case, in violation of N.C. Gen. Stat. § 75-1.1.

245. Plaintiff, North Carolina, is entitled to attorney fees and costs, penalties, and injunctive relief pursuant to N.C. Gen. Stat. § 75-1.1, *et seq*.

**Count XLIII**
**North Carolina: Data Breach Violation of N.C. Gen. Stat. § 75-65**

246. Plaintiff, North Carolina, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

247. MIE failed to notify affected individuals or others of the Data Breach as required by N.C. Gen. Stat. § 75-65.

248. As alleged in paragraphs 32 and 33, Defendants began notifying affected individuals on July 17, 2015 and did not conclude until December 2015. The effective notice date range after the breach was discovered was between 52 days and six months.

249. By waiting between 52 days and six months to notify affected individuals, Defendants violated N.C. Gen. Stat. § 75-65.

250. Plaintiff, North Carolina, is entitled to attorney fees and costs, penalties, and injunctive relief pursuant to N.C. Gen. Stat. § 75-1.1, *et seq*.

**Count XLIV**
**Tennessee: Violation of HIPAA Safeguards**

251. Plaintiff, Tennessee, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

252. Defendants' conduct constitutes violations of Administrative Safeguards, Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

a. MIE failed to review and modify security measures needed to continue the provision of reasonable and appropriate protection of ePHI in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.306(e).

b. MIE failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI that it maintained in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

c. MIE failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B).

d. MIE failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and Security Incident tracking reports in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

e. MIE failed to implement policies and procedures that, based upon its access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process that includes ePHI in accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

f. MIE failed to implement policies and procedures to address Security Incidents, including suspected Security Incidents, to mitigate, to the extent practicable, harmful effects of security incidents known to MIE, or to document such Incidents and their outcomes in accordance with the implementation specifications of the Security Rule, 45 C.F.R. § 164.308(a)(6)(ii).

g. MIE failed to assign a unique name and/or number for identifying and tracking user identity in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(iv).

i. MIE failed to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI, in violation of 45 C.F.R. § 164.312(b).

j. MIE failed to implement procedures to verify that a person or entity seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(d).

k. MIE failed to adhere to the Minimum Necessary Standard when using or disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

253. Plaintiff, Tennessee, is entitled to certain statutory damages pursuant to 42 U.S.C. 1320d-5(d)(2).

**Count XLV**
**Tennessee: Deceptive Acts in Violation of the Tennessee Consumer Protection Act, Tenn. Code § 47-18-101 *et seq*.**

254. Plaintiff, Tennessee, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

255. The Defendants' conduct constitutes a violation of Tenn. Code § 47-18-104.

256. The information security failings outlined in paragraphs 30 through 44 constitute unfair or deceptive acts in violation of Tenn. Code § 47-18-104(a), (b)(5), (7), and (27).

257. MIE committed an unfair or deceptive act by representing that it maintained appropriate Administrative and Technical Safeguards to protect patients' ePHI, and other appropriate measures to protect consumers' sensitive information, when such was not the case, in violation of Tenn. Code § 47-18-104(a), (b)(5), (7), and (27).

258. Plaintiff, Tennessee, is entitled to civil penalties pursuant to Tenn. Code § 47-18-108(b)(3), attorney fees and costs pursuant to Tenn. Code § 47-18-108(b)(4), and injunctive relief pursuant to Tenn. Code § 47-18-108(a)(1).

**Count XLVI**
**Tennessee: Data Breach Violation of Tenn. Code § 47-18-2107**

259. Plaintiff, Tennessee, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

260. MIE failed to notify affected individuals or others of the Data Breach as required by Tenn. Code Ann. § 47-18-2107.

261. As alleged in paragraphs 32 and 33, Defendants began notifying affected individuals on July 17, 2015 and did not conclude until December 2015. The effective notice date range after the breach was discovered was between 52 days and six months.

262. By waiting between 52 days and six months to notify affected individuals, Defendants violated Tenn. Code Ann. § 47-18-2107(b).

263. Plaintiff, Tennessee, is entitled to civil penalties pursuant to Tenn. Code Ann. §§ 47-18-2106 and 47-18-108(b)(3), attorney fees and costs pursuant to Tenn. Code Ann. §§ 47-18-2105(f), 47-18-2106 and 47-18-108(b)(4), and injunctive relief pursuant to Tenn. Code Ann. §§ 47-18-2105(c), 47-18-2106 and 47-18-108(a)(4).

**Count XLVII**
**Tennessee: Failure to Make Reasonable Efforts to Protect Personal Information in Violation of Tenn. Code § 47-18-2110**

264. Plaintiff, Tennessee, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

265. Defendants failed to implement and maintain reasonable procedures to protect and safeguard the unlawful disclosure of personal information in violation of Tenn. Code § 47-18-2110(a) and (d).

266. The information security failings outlined in paragraphs 30 through 40 constitute unreasonable safeguard procedures in violation of Tenn. Code § 47-18-2110(a) and (d). Plaintiff, Tennessee, is entitled to civil penalties pursuant to Tenn. Code §§ 47-18-2110(d), 47-18-2106, and 47-18-108(b)(3), attorney fees and costs pursuant to Tenn. Code §§ 47-18-2110(d), 47-18-2105(f), 47-18-2106, and 47-18-108(b)(4), and injunctive relief pursuant to Tenn. Code §§ 47-18-2110(d), 47-18-2105(c), 47-18-2106, and 47-18-108(a)(1).

**Count XLVIII**
**West Virginia: Violation of HIPAA Safeguards**

267. Plaintiff, West Virginia, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

268. Defendants' conduct constitutes violations of Administrative Safeguards, Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

a. MIE failed to review and modify security measures needed to continue the provision of reasonable and appropriate protection of ePHI in accordance with the

implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.306(e).

b. MIE failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI that it maintained in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

c. MIE failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B).

d. MIE failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and Security Incident tracking reports in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

e. MIE failed to implement policies and procedures that, based upon its access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process that includes ePHI in accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

f. MIE failed to implement policies and procedures to address Security Incidents, including suspected Security Incidents, to mitigate, to the extent practicable, harmful effects of security incidents known to MIE, or to document such Incidents and their outcomes in accordance with the implementation specifications of the Security Rule, 45 C.F.R. § 164.308(a)(6)(ii).

g. MIE failed to assign a unique name and/or number for identifying and tracking user identity in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(iv).

i. MIE failed to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI, in violation of 45 C.F.R. § 164.312(b).

j. MIE failed to implement procedures to verify that a person or entity seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

k. MIE failed to adhere to the Minimum Necessary Standard when using or disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

269. Plaintiff, West Virginia, is entitled to certain statutory damages pursuant to 42 U.S.C. 1320d-5(d)(2).

**Count XLIX**
**West Virginia: Deceptive Acts in Violation of W. Va. Code § 46A-6-104**

270. Plaintiff, West Virginia, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

271. The Defendants' conduct constitutes a violation of W. Va. Code § 46A-6-104.

272. The information security failings outlined in paragraphs 23 through 44 constitute unfair or deceptive acts in violation of W. Va. Code § 46A-6-104.

273. MIE committed an unfair or deceptive act by representing that it maintained appropriate Administrative and Technical Safeguards to protect patients' ePHI, and other appropriate measures to protect consumers' sensitive information, when such was not the case, in violation of W. Va. Code § 46A-6-104.

274. Plaintiff, West Virginia, is entitled to civil penalties pursuant to W.Va. Code § 46A-7-111, attorney fees and costs pursuant to W.Va. Code § 46A-7-108, and injunctive relief pursuant to W.Va. Code § 46A-7-108.

**Count L**
**Wisconsin: Violation of HIPAA Safeguards**

275. Plaintiff, Wisconsin, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

276. Defendants' conduct constitutes violations of Administrative Safeguards, Technical Safeguards, and implementation specifications as required by HIPAA. Specifically:

a. MIE failed to review and modify security measures needed to continue the provision of reasonable and appropriate protection of ePHI in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.306(e).

b. MIE failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI that it maintained in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

c. MIE failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in accordance with the

implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B).

d. MIE failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and Security Incident tracking reports in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

e. MIE failed to implement policies and procedures that, based upon its access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process that includes ePHI in accordance with 45 C.F.R. § 164.308(a)(4)(ii)(C).

f. MIE failed to implement policies and procedures to address Security Incidents, including suspected Security Incidents, to mitigate, to the extent practicable, harmful effects of security incidents known to MIE, or to document such Incidents and their outcomes in accordance with the implementation specifications of the Security Rule, 45 C.F.R. § 164.308(a)(6)(ii).

g. MIE failed to assign a unique name and/or number for identifying and tracking user identity in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(i).

h. MIE failed to implement a mechanism to encrypt and decrypt ePHI, in accordance with the implementation specifications of the Security Rule. 45 C.F.R. § 164.312(a)(2)(iv).

i. MIE failed to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI, in violation of 45 C.F.R. § 164.312(b).

j. MIE failed to implement procedures to verify that a person or entity seeking access to ePHI is the one claimed, in violation of 45 C.F.R. § 164.312(c)(2)(d).

k. MIE failed to adhere to the Minimum Necessary Standard when using or disclosing ePHI, in violation of 45 C.F.R. § 164.502(b)(1).

277. Plaintiff, Wisconsin, is entitled to certain statutory damages pursuant to 42 U.S.C. 1320d-5(d)(2).

**Count LI**
**Wisconsin: Fraudulent Representations in Violation of Wis. Stat. § 100.20**

278. Plaintiff, Wisconsin, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

279. The Defendants' conduct constitutes a violation of Wis. Stat. § 100.18.

280. MIE represented that it maintained appropriate Administrative and Technical Safeguards to protect patients' ePHI, and other appropriate measures to protect consumers' sensitive information, when such was not the case, in violation of Wis. Stat. § 100.18.

281. Plaintiff, Wisconsin, is entitled to civil penalties, attorney's fees and costs, and injunctive relief pursuant to Wis. Stat. §§ 100.26 and 93.20.

**Count LII**
**Wisconsin: Negligent Disclosure of Patient Health Care Records in Violation of Wis. Stat. § 146.84(2)(b)**

282. Plaintiff, Wisconsin, incorporates the factual allegations in paragraphs 1 through 44 of this Complaint.

283. The Defendants negligently disclosed confidential information in violation of Wis. Stat. § 146.82.

284. Plaintiff, Wisconsin, is entitled to civil penalties pursuant to Wis. Stat. § 146.84(2)(b).

**THIS COURT'S POWER TO GRANT RELIEF**

285. Pursuant to 28 U.S.C. § 1367, this Court has supplemental jurisdiction to allow the Plaintiff States to enforce their state laws against Defendants in this Court and to grant such relief as provided under the following state laws including injunctive relief, civil penalties, attorneys' fees, expenses, costs, and such other relief to which the Plaintiff States may be entitled:

| State | Deceptive Acts | Data Breach | PIPA |
|---|---|---|---|
| Arizona: | Ariz. Rev. Stat. §§ 44-1528, 44-1534, and 44-1531 | | |
| Arkansas: | Ark. Code Ann. § 4-88-113 | Ark. Code Ann. §§ 4-110-108 and 4-88-101 *et seq*. | Ark. Code Ann. §§ 4-110-108 and 4-88-101 *et seq*. |
| Connecticut: | Conn. Gen. Stat. § 42-110b, *et seq*. | Conn. Gen. Stat. § 36a-701b | Conn. Gen. Stat. § 42-471 |
| Florida: | Sections 501.207, 501.2075, and 501.2105, Florida Statutes | Section 501.171(9), Florida Statutes | Section 501.171(9), Florida Statutes |
| Indiana: | Ind. Code §§ 24-5-0.5-4(C), and 24-5-0.5-4(G) | | Ind. Code § 24-4.9-3-3.5(f) |
| Iowa: | Iowa Code § 714.16 | Iowa Code § 715c.2 | |
| Kansas: | Kan. Stat. §§ 50-632, and 50-636 | Kan. Stat. § 50-7a02 | Kan. Stat. § 50-6139b |
| Kentucky: | Ky. Rev. Stat. §§ 367.110-.300, and 367.990 | | |

| | | | |
|---|---|---|---|
| Louisiana: | La. Rev. Stat. § 51:1401 et seq. | La. Rev. Stat. 51:3071 et seq. | |
| Michigan: | Mich. Comp. Laws § 445.905 | Mich. Comp. Laws § 445.72(13) | |
| Minnesota: | Minn. Stat. § 8.31 | Minn. Stat. § 8.31 | |
| Nebraska: | Neb. Rev. Stat. §§ 59-1602; 59-1608, and 59-1614 | Neb. Rev. Stat. § 87-806 | |
| North Carolina | N.C. Gen. Stat. § 75-1.1, *et seq*. | N.C. Gen. Stat. § 75-65 | N.C. Gen. Stat. § 75-60, *et seq*. |
| Tennessee: | Tenn. Code § 47-18-108 | Tenn. Cod Ann. §§ 47-18-2105, 47-18-2016 | Tenn. Code §§ 47-18-2110, 47-18-2105, and 47-18-2016 |
| West Virginia: | W.Va. Code §§ 46A-1-101 *et seq*., 46A-7-108, and 46A-7-111 | | |
| Wisconsin: | Wis. Stat. §§ 93.20, 100.18, and 100.26 | | Wis. Stat. § 146.84(2)(b) |

## PRAYER FOR RELIEF

WHEREFORE, the Plaintiff States respectfully request that the Court:

A. Award Plaintiffs such injunctive relief as permitted by statute;

B. Award Plaintiffs a financial judgment for restitution and civil penalties as permitted by statute, and;

C. Award Plaintiffs such other relief the Court deems just and proper.

Respectfully Submitted,

Date: _____

Curtis T. Hill Jr.

Attorney General of Indiana

Atty. No. 13999-20

By: */s/ Michael A. Eades*
Michael A. Eades, Deputy Attorney General
Atty. No. 31015-49

By: */s/ Douglas S. Swetnam*
Douglas S. Swetnam, Section Chief
Atty. No. 15860-49

Data Privacy and Identity Theft Unit
Office of the Attorney General
302 West Washington St., 5th Floor
Indianapolis, IN 46204
Tel: (317) 233-3300
Michael.Eades@atg.in.gov
Douglas.Swetnam@atg.in.gov

Attorney General Mark Brnovich

By: */s/* John C. Gray
John C. Gray (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Mark Brnovich
2005 N. Central Ave.
Phoenix, AZ 85004
Email: John.Gray@azag.gov
Telephone: (602) 542-7753
Attorney for Plaintiff State of Arizona

Attorney General Leslie Rutledge

By: /s/ Peggy Johnson
Peggy Johnson (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Leslie Rutledge
323 Center St., Suite 200
Little Rock, AR 72201
Email: peggy.johnson@arkansasag.gov
Telephone: (501) 682-8062
Attorney for Plaintiff State of Arkansas

Attorney General William Tong

By: /s/ Michele Lucan
Michele Lucan (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General William Tong
110 Serman Street
Hartford, CT 06105
Email: michele.lucan@ct.gov
Telephone: (860) 808-5440
Attorney for Plaintiff State of Connecticut

Attorney General Ashley Moody

By: /s/ Diane Oates
Diane Oates (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Ashley Moody
110 Southeast 6th Street
Fort Lauderdale, FL 33301
Email: Diane.Oates@myfloridalegal.com
Telephone: (954) 712-4603
Attorney for Plaintiff State of Florida

By: /s/ Patrice Malloy
Patrice Malloy (Pro Hac Vice)
Bureau Chief, Multistate and Privacy Bureau
Florida Office of the Attorney General
110 SE 6th Street
Fort Lauderdale, FL 33301
(954) 712-4669
Patrice.Malloy@myfloridalegal.com

Attorney General Tom Miller

By: /s/ William Pearson
William Pearson (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Tom Miller
1305 E. Walnut, 2nd Floor
Des Moines, IA 50319
Email: William.Pearson@ag.iowa.gov
Telephone: (515) 281-3731
Attorney for Plaintiff State of Iowa

Attorney General Derek Schmidt

By: /s/ Sarah Dietz
Sarah Dietz (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Derek Schmidt
120 S.W. 10th Ave., 2nd Floor
Topeka, KS 66612
Email: sarah.dietz@ag.ks.gov
Telephone: (785) 368-6204
Attorney for Plaintiff State of Kansas

Attorney General Andy Beshear

By: /s/ Kevin R. Winstead
Kevin R. Winstead (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Andy Beshear
1024 Capital Center Drive
Frankfort, KY 40601
Email: Kevin.Winstead@ky.gov
Telephone: (502) 696-5389
Attorney for Plaintiff Commonwealth of Kentucky

Attorney General Jeff Landry

By: /s/ Alberto A. De Puy
Alberto A. De Puy (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Jeff Landry
1885 N. Third St.
Baton Rouge, LA 70802
Email: DePuyA@ag.louisiana.gov
Telephone: (225) 326-647

By: /s/ L. Christopher Styron
L. Christopher Styron (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Jeff Landry
1885 N. Third St.
Baton Rouge, LA 70802
Email: styronl@ag.louisiana.gov
Telephone: (225) 326-6400
Attorneys for Plaintiff State of Louisiana

Attorney General Dana Nessel

By: /s/ Kathy Fitzgerald
Kathy Fitzgerald (Pro Hac Vice)
Assistant Attorney General
Department of Attorney General Dana Nessel
Corporate Oversight Division
525 W. Ottawa St., 5th Floor
Lansing, MI 48933
Email: fitzgeraldk@michigan.gov
Telephone: (517) 335-7632
Attorney for Plaintiff State of Michigan

Attorney General Keith Ellison

By: /s/ Jason T. Pleggenkuhle
Jason T. Pleggenkuhle (Pro Hac Vice)
Assistant Attorney General
Office of Attorney General Keith Ellison
Bremer Tower, Suite 1200
445 Minnesota St.
St. Paul, MN 55101-2130
Email: jason.pleggenkuhle@ag.state.mn.us
Telephone: (651) 757-1147
Attorney for Plaintiff State of Minnesota

Attorney General Doug Peterson

By: /s/ Daniel J. Birdsall
Daniel J. Birdsall (Pro Hac Vice)
Assistant Attorneys General
Office of Attorney General Doug Peterson
2115 State Capitol
PO Box 98920
Lincoln, NE 68509
Email: dan.birdsall@nebraska.gov
Telephone: (402) 471-1279
Attorney for Plaintiff State of Nebraska

Attorney General Joshua H. Stein

By: /s/ Kimberley A. D'arruda
Kimberley A. D'Arruda (Pro Hac Vice)
Special Deputy Attorney General
North Carolina Department of Justice
Office of Attorney General Joshua H. Stein
P.O. Box 629
Raleigh, NC 27602-0629
Email: kdarruda@ncdoj.gov
Telephone: (919) 716-6013
Attorney for Plaintiff State of North Carolina

Attorney General Herbert Slattery III

By: /s/ Carolyn U. Smith
Carolyn U. Smith (Pro Hac Vice)
Senior Assistant Attorney General
Office of the Attorney General and Reporter Herbert H. Slattery III
P.O. Box 20207

Nashville, TN 37202-0207
Email: Carolyn.smith@ag.tn.gov
Telephone: (615) 532-2578
Attorney for Plaintiff State of Tennessee

Attorney General Patrick Morrisey

By: /s/ Tanya L. Godfrey
Tanya L. Godfrey (Pro Hac Vice)
Assistant Attorney General
Office of the West Virginia Attorney General Patrick Morrisey
269 Aikens Center
Martinsburg, WV 25404
Email: tanya.l.godfrey@wvago.gov
Telephone: (304) 267-0239
Attorney for Plaintiff State of West Virginia

Attorney General Josh Kaul

By: /s/ R. Duane Harlow
R. Duane Harlow (Pro Hac Vice)
Assistant Attorney General
Director, Consumer Protection and Antitrust Unit
Wisconsin Department of Justice
Office of Attorney General Josh Kaul
17 W. Main St., P.O. Box 7857
Madison, WI 53707-7857
Email: HarlowRD@doj.state.wi.us
Telephone: (608) 266-2950
Attorney for Plaintiff State of Wisconsin

**CERTIFICATE OF SERVICE**

I certify that on May 23, 2019 a copy of this document was served on all counsel of record by operation of the Court's electronic filing system.

*/s/ Michael A. Eades*
Michael A. Eades, Deputy Attorney General
Data Privacy and Identity Theft Unit
Office of the Indiana Attorney General